Acceleration axis selection in biometric technique based on gesture recognition

J. Guerra Casanova, C. Sánchez Ávila, A. de Santos Sierra, G. Bailador del Pozo and V. Jara Vera
Grupo de Biometría y Tratamiento Numérico de la Información
Centro de Domótica Integral (CeDInt-UPM), Universidad Politécnica de Madrid
Pozuelo de Alarcón, Madrid, Spain
Email: {jguerra, csa, alberto, gbailador, vjara}@cedint.upm.es

***Abstract*—This article proposes a biometric technique based on gesture recognition performed directly in a mobile device embedding an accelerometer. As time consumption is an essential requirement, this article aims to discover the most distinctive acceleration axis information in order to find the best strategy considering EER and consumed time. Best EER result of 2.5% has been obtained when the information of accelerations on each of the three axis is analyzed. When reducing the information inspected to only two or one acceleration axis signals, EER values are 2.98% and 4.34% respectively. Preprocessing various acceleration signals by calculating their magnitude outcomes with higher EER values. All this work has been developed from a database of 34 individuals who have performed their identifying gestures, and three falsifiers who have attempted to forge each original in-air signatures from studying video records.**

I. Introduction

Gesture recognition is an important field of investigation where the main task is to identify a specific gesture performed by anyone in order to effectuate an expected action as a response to this gesture [1]. In this work, we propose a novel biometric technique based on the utilization of gestures as a manner to identify people.

Nowadays, most people make use of mobile phones that provide access to applications where there is an authentication requirement. Remembering and repeating alphanumeric passwords is still the most usual technique to assure the identity of a person in a mobile device. But these techniques are not secure enough, as these passwords can be guessed, copied or stolen. In this mobile context, biometrics raises again as a method to ensure identities. Some works trying to join classical biometric techniques in a mobile scenario have been already developed, based on iris recognition [2], face recognition [3], voice recognition [4] or keystroke [5].

In this article, we propose a technique to authenticate a person based on gesture recognition. A person is authenticated when he/she performs an identifying gesture in the air holding a mobile device. This identifying gesture is considered as an in-air signature, that in spite of other people may watch the performance of the gesture, they are not able to reproduce it in the same way as the original user. We assume that every person is able to perform a gesture in the air in a distinctive way depending on physical characteristics as length of the arm, size of the hand holding the device, capability of turning the wrist or muscle strength.

The movement of the hand when carrying out the in-air signature is extracted by an accelerometer embedded in the mobile phone at a sampling rate of 10ms, frequency precise enough to get representative signals of a hand movement in the air [6]. Besides, there is a growing number of mobile phones embedding an accelerometer in the market [7], so this technique may be easily extended in a short future.

This proposal of in-air signature technique is similar to the traditional handwritten signature [8], but adapted to a mobile environment. In this approach, feature extraction is directly performed within an own mobile device without any additional device requirement. Besides, all the authentication algorithms are executed inside the device, without any additional device or server. This characteristic of compactness may be useful to cryptobiometric systems, where a cryptographic key is released or generated from biometric authentication [9], [10].

Executing the algorithms of authentication directly in the mobile device implies time restriction, so it is important to find the best strategy to process all the information in a short period of time in order to be a "real-time" authentication technique. To fulfill this aim, it is needed to find the most distinctive information inside an in-air signature.

This article aims to accomplish this task, studying which axis of acceleration includes the most distinctive information in an in-air signature performed with a mobile phone. As a result of this work, a reduction of information needed to authenticate a user may be considered in order to reduce the consumption time required to effectuate the process as well.

This article is divided in the following Sections. Firstly, Section II describes briefly the mathematical method utilized to analyze the different accelerations signals of each performance of an in-air signature. To support the experiments of the article, a database of 34 different in-air signatures has been developed. In Section III, the procedure of obtaining the database is explained. Then, Section IV describes the different experiments and results obtained when different axis accelerations signals proceeding from the in-air signature database are analyzed in order to find the most distinctive information. Finally, in Section V conclusions of this work are summarized.

II. Analysis procedure

In this article, an algorithm based on Dynamic Programming [11] has been developed to find the best alignment between two signals, in order to be able to elucidate whether a sample is truthful or not.

Despite a user performs the same gesture holding the mobile device in the same way, there will be always some little variations on the speed and manner the user carries out his/her in-air signature. From this alignment algorithm those little deviations are corrected without compensating high differences.

For that purpose, the algorithm includes a fuzzy function in the diagonal movement of the score equation [12], when two points of the sequences are considered best aligned. The proposed score function is shown in Equation 1, and it is calculated for each point of the two signals.

$$s_{i,j} = \max \begin{cases} s_{i,j-1} + g \\ s_{i-1,j-1} + \Delta \\ s_{i-i,j} + g \end{cases} \quad (1)$$

where g is a constant, known as gap penalty [11], whose value is obtained to maximize the overall performance, and Δ is a fuzzy decision function that represents a Gaussian distribution as in Equation 2:

$$\Delta = e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (2)$$

where μ and x are the values of the previous points in base to whom the score of the new points (i, j) are calculated. Finally, σ is a constant stating to what extend two these values are similar.

Once the score function is calculated for each point of the two signals desired to be best aligned, a backtracking algorithm is executed to find the path that maximizes the overall score function. Any vertical or horizontal movements implies adding a zero value on one of the sequences, and interpolating this point later. As a result of this algorithm, signals length is duplicated. When the alignment of the signals is accomplished, Euclidean distance is calculated in order to measure the differences between aligned signals. Consequently, a numerical value is obtained at the end of the analysis process; the lower the value is, the more similar the analyzed signals are, and viceversa.

III. Acquisition of an in-air Signature Biometric Database

The in-air signature biometric technique has been validated applying the algorithm explained in Section II over a database of 34 gestures of different users. This database has been obtained in two different sessions:

In the first session, 34 volunteers (from ages 19 to 60, 15 women and 19 men) have performed the gesture they would choose as their in-air biometric signature in this technique holding a device embedding an accelerometer. Specifically, an application for iPhone 3G has been developed to extract the accelerations of the movement of the hand on each axis X-Y-Z while carrying out a gesture at a sampling rate of 10 ms. Some instructions have been provided to encourage the volunteers to perform remindful and complex enough gestures so that anyone except themselves may reproduce it immediately.

Each user has repeated 7 times his/her gesture, with intervals of 10 seconds to reduce dependence between samples. Furthermore, all of these sessions of performing new gestures have been recorded on video, so that other users may try to forge the gestures of someone else by watching and studying these videos.

In the second session, three different people have tried to forge each of the 34 original in-air biometric signatures by studying the videos recorded in the previous session. The same feature extraction application and the same mobile device have been utilized to extract the accelerations of the falsification signatures at the same sampling rate of 10 ms.

An evaluation of the feasibility of the technique has been developed from all the original and falsified samples of gestures obtained in both sessions. The explanation of the experiments carried out for this aim, and the results obtained are shown in next Section.

IV. Experimental Results

The biometric database described in the previous Section yields in 238 (34 users, 7 samples each) original and 714 impostor (34 users, 3 forgers, 7 samples each) samples of gestures. Each sample is composed as well by three signals corresponding to the acceleration on each axis X-Y-Z. In this work, X axis represents the left-right direction, Y axis denotes movements up and down and Z axis stands for accelerations to the front and the back.

Three original samples of each gesture chosen randomly have been considered as the in-air signature biometric template; the other four original samples represent truthful attempts of verification that should be accepted. All impostor samples symbolize false trials that should be rejected.

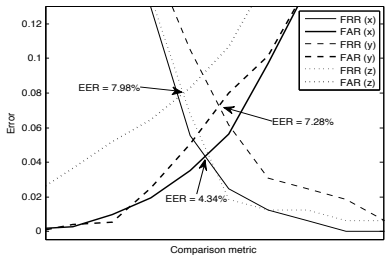
Each accessing attempt consists of executing the algorithm explained in Section II between the accessing sample and each of the samples that compose the biometric template.

Consequently, Equal Error Rates (EER) [13] have been calculated in this article from 136 (34 users, 4 accessing samples each) truthful samples in order to obtain FRR (False Rejection Rate) and 714 (34 users, 3 forgers, 7 samples each) impostor access samples to determine FAR (False Acceptance Rate).

This Section is organized according to the number of signals required to execute each experiment. For each experiment, $T_E(l)$ denotes the execution time of the algorithm, which depends on the length of the signals analyzed. Moreover, L represents the length of the signals of acceleration in each axis.

All the experiments have been carried out in a Mac Computer (2.4G Ghz, 1Gb RAM) but the measurements of time of the algorithm in different conditions have been obtained directly from processing the signals in a specific mobile device embedding an accelerometer (an iPhone). The time

Fig. 1. Resulting EER analyzing one acceleration axis.



consumption of an algorithm has been measured as the average time of 10 consecutive executions of signals of length 600 corresponding to a in-air signature of 6 seconds.

A. Experiment with acceleration signals in one axis

In this subsection the behavior of the system is studied when only signals of one axis are considered. As there is only one signal involved it means that, the lower EER results, the most distinctive information the accelerometer axis contains.

Figure 1 presents EER results obtained when only one accelerometer axis signal is analyzed. It can be observed that the accelerometer axis that carries the most distinguishing information alone is X, as an Equal Error Rate of 4.34% is obtained. Evaluating axes Y and Z provide Equal Error Rates of 7.28% and 7.98% respectively, much worse than the other. In conclusion, the most distinctive axis of in-air signature accelerations is X (left-right direction). The required time of this analysis measured directly in a mobile phone is 1.505 seconds, equivalent to one execution of the algorithm with signals of length L ($T_E(L)$).

B. Experiment with acceleration signals in two axes

In this Subsection, experiments are carried out including two axis of the acceleration when performing the gesture. Each figure of results of every experiment studied in this section presents together the consequences of analyzing X-Y, X-Z and Y-Z separately. These experiments increase time consumption respect to the previous ones, when only one acceleration axis signal was analyzed, but reduce Equal Error Rates.

In this scenario the algorithm is executed twice, one for each signal analyzed separately. Consequently, the time needed for this experiment is equivalent to execute twice the algorithm with two signals of length L ($2T_E(L)$), which is obviously, the double of the time consumed in the previous experiment.

The fusion of the information of each axis is performed at decision level. The average of the results of the algorithm execution on each axis is considered as the final value of decision. With these hypothesis, an Equal Error Rate of 2.98%, 4.35% or 4.29% is obtained analyzing signals X-Y, X-Z and Y-Z respectively. (Figure 2)

According to these results, the best selection of acceleration axes is X and Y, as the lowest EER is obtained with them. In the previous experiment it was deducted that the most distinctive axis is X which is in consonant with the results obtained in this experiment. Furthermore, a new conclusion can be extracted as adding information of axis Y to axes X

Fig. 2. Resulting EER analyzing two acceleration axis.

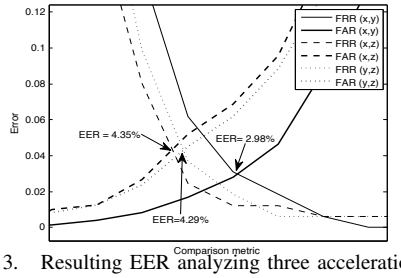
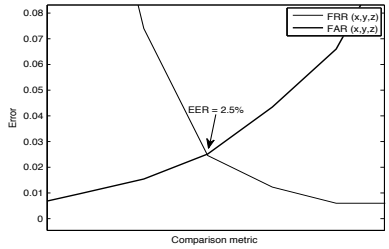


Fig. 3. Resulting EER analyzing three acceleration axis



improves much more EER rather than utilizing axis Z instead. Besides, only at duplicating consumption time, EER has been reduced from 4.38% to 2.98%, so for real applications it seems a much better strategy.

C. Experiment with acceleration signals in three axes

In this experiment, accelerations on axis X, Y and Z is analyzed, which is all the information obtained from each sample of each in-air signature.

In this scenario, the algorithm is executed three times, one for each axis signal separately, so consumption time is equivalent to three times the execution of the algorithm with two signals of length L ($3T_E(L)$), which means 4.15 seconds in a real mobile phone.

The information is fused at decision level, as in previous experiments, by calculating the average of the result of each process of each signal. In these conditions an Equal Error Rate of 2.5% has been obtained. (Figure 3)

According to this result, the lowest EER obtained with this in-air signature is 2.5%, when all the information extracted is involved. Comparing with the previous experiment, reader should notice that adding information of acceleration in axis Z only improves EER in 0.48% altough consumption time increases 1.5 seconds. This low improvement must be considered in applications where time response is more critical than a higher security, as a solution with accelerations in axes X and Y offers already good results in a shorter time.

D. Experiments with one signal obtained from preprocessing several acceleration axes

Another scenario should be studied, where information of various axes is fused before executing the algorithm. Calculating the magnitude of a signal with various axes would seem to be a good solution, as information of all the axes is considered and only a consumption time equivalent to one execution of the algorithm with signals of length L is required ($T_E(L)$).

Fig. 4. Resulting EER calculating the magnitude of two acceleration axis.

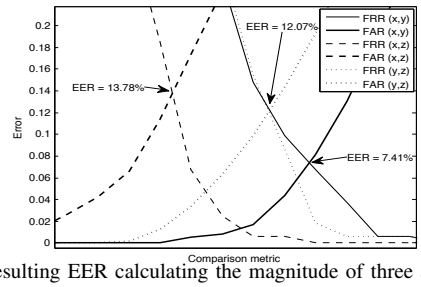
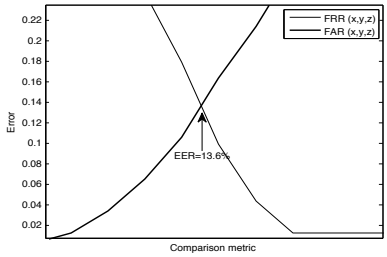


Fig. 5. Resulting EER calculating the magnitude of three acceleration axis.



Unfortunately, when the magnitude of several acceleration axis signals is calculated, higher EER results are obtained.

Results when the magnitude has been calculated from two acceleration axes can be observed in Figure 4. The lowest EER obtained is 7.41%, corresponding with information of axes X and Y. This result is consistent with previous experiments, as this combination of information is still the one that carries the most disctintive information. Moreover, it can be concluded that magnitude operation is not a good method for this purpose. On the other hand, analyzing other combinations of two signals EER of 13.78% and 12.07% has been obtained from X-Z and Y-Z signals respectively.

If the magnitude of the three acceleration axis signals is calculated, results become even worse (Figure 5). An EER of 13.6% is obtained, which is almost the worst result obtained in the study. Consequently, it can be deducted that when the magnitude of several signals is calculated, disctintive information is not separated but intermingled, so distinguising between in-air signatures becomes even more difficult producing a larger amount of errors.

V. Conclusions

In this article, a biometric technique based on in-air signatures has been introduced in order to authenticate a person in a mobile device. A biometric database, composed by 34 original in-air signatures and 21 falsification attempts for each, has been created to study the viability of this technique.

The lower Equal Error Rate obtained is 2.5% when accelerations in the three axes are consired. The best EER result analyzing only two axis signals is 2.98% obtained from the combination of axes X and Y. Other two-signal combinations deteriorate EER. When only one axis is examined, the lowest EER is 4.34%, obtained from axis X. Axes Y and Z do not approach this result. Other solutions, based on preprocessing several accelerometer signals by calculating their magnitude, have obtained much higher EER results. Consequently, it has been proved that a magnitude method is not a good solution in this scenario.

In conclusion, the best strategy depends on the time consumption requirement. If time is critical, a solution where acceleration in axis X is selected to be analyzed appears to be the most convenient; otherwise, selecting X and Y accelerations offers almost an optimal error rates saving some execution time. If the most secure strategy is need without taking in consideration time requirement, the adopted solution would be the obvious, utilizing all the information extracted.

References

[1] J. Daugman, "Face and gesture recognition: Overview," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, pp. 675–676, 1997.

[2] D. ho Cho, K. R. Park, D. W. Rhee, Y. Kim, and J. Yang, "Pupil and iris localization for iris recognition in mobile phones," *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, International Conference on & Self-Assembling Wireless Networks, International Workshop on*, vol. 0, pp. 197–201, 2006.

[3] Q. Tao and R. Veldhuis, "Biometric authentication for a mobile personal device," *Mobile and Ubiquitous Systems, Annual International Conference on*, vol. 0, pp. 1–3, 2006.

[4] H. A. Shabeer and P. Suganthi, "Mobile phones security using biometrics," *Computational Intelligence and Multimedia Applications, International Conference on*, vol. 4, pp. 270–274, 2007.

[5] S. seob Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Computers and Security*, vol. 28, no. 1-2, pp. 85 – 93, 2009.

[6] C. Verplaetse, "Inertial proprioceptive devices: self-motion-sensing toys and tools," *IBM Syst. J.*, vol. 35, no. 3-4, pp. 639–650, 1996.

[7] J. H. Steve Dowling, Nancy Paxton, "Apple reports first quarter results," Apple Inc., Tech. Rep., 2009. [Online]. Available: http://www.apple.com/pr/library/2009/01/21results.html

[8] A. J. Friederike, A. K. Jain, F. D. Griess, S. D. Connell, E. Lansing, and M. J, "On-line signature verification," *Pattern Recognition*, vol. 35, 2002.

[9] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, 2006.

[10] S. Chikkerur, V. Chavan, and V. Govindaraju, "A study on the convergence of biometrics and cryptography," in *Workshop on Secure Knowledge Management,Buffalo*, 2004.

[11] W. Miller, "An introduction to bioinformatics algorithms. neil c. jones and pavel a. pevzner," *Journal of the American Statistical Association*, vol. 101, pp. 855–855, June 2006. [Online]. Available: http://ideas.repec.org/a/bes/jnlasa/v101y2006p855-855.html

[12] A. de Santos Sierra, C. Avila, and V. Vera, "A fuzzy dna-based algorithm for identification and authentication in an iris detection system," in *Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on*, Oct. 2008, pp. 226–232.

[13] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.